AMENDMENTS TO THE SPECIFICATION

Please amend paragraph **0048** by replacing it with the following:

[0048] The background digits of the example ACI can be read in the background of a document "behind" other alphanumeric indicia. In a particularly advantageous arrangement of the example ACI, some of the background digits are oriented perpendicular to the main orientation of the document. In another particularly advantageous arrangement of the example ACI, small background digits fill a substantial portion of one or more document signature, stamp, and/or annotation fields. In the example, the small background digits are in the signature fields where ~~"void"is~~ "void" is handwritten in ~~pace~~ place of actual signatures.

Please amend paragraph **0049** by replacing it with the following:

[0049] Background digits according to various aspects of the inventions advantageously maintain a contextual thread between (1) inked indicia (e.g., one or more holographic signatures, a notary stamp, etc.) in a document and (2) printed indicia elsewhere in the document, making it difficult to "lift" the image of such inked indicia and transfer it to a forged document. The background digits are preferably in an outline font to maintain readability of the main document indicia. The spacing, font size, and font type of the digits is preferably varied in a way unpredictable to a forger (e.g., pseudorandomly) to make duplication of [a] an "erasing negative" of the background digits difficult. (An erasing negative could conceivably be used to eliminate background digits and permit "lifting" of inked indicia that would otherwise have digits in its background field.)

Please amend paragraph **0050** by replacing it with the following:

[0050] As discussed above, an ACI binds a signer to a digital signature uniquely corresponding to a positively identified public key. Most fingerprints and digital signatures could conceivably correspond to multiple records. However, the likelihood of finding a corresponding electronic record other than the one of interest, given a uniform probability of obtaining all possible fingerprints of digital signatures from a given record, is usually vanishingly small. The likelihood of finding a second match that could be mistaken for the electronic record of interest is so small, in most cryptographic applications, as to be considered impossible. Embodiments are certainly possible, however, in which ~~and~~ an electronic record is considered to uniquely correspond to a fingerprint or digital signature with a higher probability of a false match.

PLEASE AMEND paragraph **0051** by replacing it with the following:

[0051] The ACI is a specific example of a positive identification of an electronic record in which the electronic record is a public signing key. (Another example in which an electronic copy of a publicly accessible paper file is positively identified by a third party who has inspected the file[,] is shown in Appendix F.) The identification employs an "integrated" combination of: (a) a code "uniquely corresponding" to that electronic record (e.g., a SHA-1 cryptographic hash code); and (b) a holographic signature ~~and~~ (or facsimile thereof). The combination is said to be integrated when it would be difficult for a forger to separate the elements of the combination. Another way of describing ~~and~~ an integrated combination of (a) and (b) is having a contextual thread between (a) and (b). (See the discussion of "background digits" above.)

PLEASE AMEND paragraph **0052** by replacing it with the following:

[0052] A paper document [of] or facsimile copy thereof containing the combination can include the following advantageous aspects: (1) the digits of the code can be printed in background digits of the document, including behind fields for handwriting, as in the above example ACI with background digits of a PGP "fingerprint"; (2) the document can include a facsimile copy of a photographic identification of the signer, which can be referenced in language of the document (e.g., a Notary's statement). For example, an ACI can include a photocopy of a driver's license.

PLEASE AMEND paragraph **0105** by replacing it with the following:

[0105] TABLE I

SC	This telephone call is being recorded for the permanent records of SelfCertify.com, for the permanent records of SelfCertify.com, for the purpose of authenticating a public key you are certifying with SelfCertify.com. If you consent to this recording and proceeding with the certification process, please state "I agree" and then recite your full legal name and mailing address.
Alice	I agree. My name is Alice P. Costas, and my address is 537 Main Street, Anytown Arizona 12345.
SC	Now that we have ~~you~~ your agreement to record this telephone call and proceed, we will ask that you carefully read that terms of the "Authentication and Certification Instrument." You will be asked to agree to the terms of that document. and your recorded verbal agreement will legally bind you to those terms as if you had signed that document with your ink signature. Please state "Yes, it is" to confirm with the statement entitled "Authentication Certification and Instrument" is now displayed on ~~you wed~~ your web browser at https (colon, double forward slash) www.selfcertify.com/aci32776 and that the document refers to a public key with fingerprint 2355 7782 1193 8001. You will be given an opportunity to read the document in a minute if you haven't already done so. Right now, we just ask you to confirm that the document is being displayed.
Alice	Yes, it is.
SC	Now we will ask you to ensure that you have read the document. We recommend that you print the document for you records, as you will be bound to its terms if you proceed. Please say "I have read the document" when you have done so.
Alice	Yes, I've read the document.
SC	Now please confirm your legally binding agreement with the terms of the document entitled "Authentication and Certification Instrument," displayed on your web browser at https (colon, double forward slash) www.selfcertify.com/aci327776 and referring to a public key with fingerprint 2355 7782 1193 8001, on this (blank) day of (blank) (blank) by stating "Yes, I agree to the terms of the document."
Alice	Yes, I agree.
SC	Sorry, you need to state exactly, "Yes, I agree to the terms of the document."

Alice	Yes, I agree to the terms of the document.
SC	Thank you. This ends your verbal certification of your public key. Thank you.

PLEASE AMEND paragraph **0112** by replacing it with the following:

[0112] The terms "virtual signature printing," "virtual signature printer" are to be broadly understood as including any mathematical construct, structure, method, system, etc., as the case may be, suitable for carrying out the function of authenticating an electronic record such as a word processor document by "printing" the document using a printer driver that does not actually produce printed output, [al] at least not as its main purpose. Instead, such a printer driver according to various aspects of the inventions creates another file that includes, or references, indicia of the user's digital signature authentication of the electronic record.

PLEASE AMEND paragraph **0152** by replacing it with the following:

[0152] An analysis of entropy using the preferred non-repeating ~~digitsin~~ digits in the system of FIGS. 13-14 is found in Appendix AB. With 7 x 5 = 35 = M choices and N = 8 non-duplicate digits, the number of possibilities X = M•(M-1)•(M-2)•(M-3)...(M-N-), which works out to X = 6.67 x 10^{14}. Based on the base 2 log of X, the result is 49.2 bits of entropy. With a 0.5 second delay between digits, d = 4 seconds, and 4X / (3600 sec./hr x 24 hr/d x 365 d/yr) = 84,496,818 years.

PLEASE AMEND paragraph **0177** by replacing it with the following:

[0177] The pseudogroup operation will now be ~~discussedin~~ discussed in more detail with reference to FIGS. 18-20.

PLEASE AMEND paragraph **0199** by replacing it with the following:

[0199] Systems according to various aspects of the invention can be useful in the legal profession where sometimes legal professionals are called upon to testify about matters that were assumed to be privileged but the court determines that they are not for whatever reason, as happens in patent practice sometimes. If an attorney or agent has communicated with his client using this system, and the client agrees to destroy the passphrase after the matter is complete, and the ~~device~~ advice communicated by the attorney or agent is no longer relevant or needed and has been acted upon completely, then it is impossible for any court or any party to discover what [to] the parties discussed.

PLEASE AMEND paragraph **0208** by replacing it with the following:

[0208] In the process[f] flow illustrated in FIG. 21, a sensitive message 2112, which is never saved, preferably, comes from a sender/originator 2110. Encrypt 2114 uses a temporary key 2122, which is destroyed after a period "X."